COURSE TITLE	**CYBER LAW AND ETHICS**
COURSE CODE	**01CC0507**
COURSE CREDITS	**3**

Objective:

1 .Understanding Legal Frameworks to familiarize students with the legal principles, regulations, and frameworks that govern cyberspace and digital technologies. Exploring Ethical Issues to examine ethical dilemmas and considerations arising from the use of technology, digital communications, and data handling practices. Analyzing Cybersecurity Challenges to analyze cybersecurity threats, vulnerabilities, and measures within the context of legal and ethical frameworks. Examining Digital Rights to explore issues related to digital rights, freedom of expression online, censorship, surveillance, and the balance between security and privacy in cyberspace. Applying Legal and Ethical Principles to develop skills in applying legal and ethical principles to real-world scenarios involving digital technologies, data breaches, intellectual property disputes, and regulatory compliance.

Course Outcomes: After completion of this course, student will be able to:

1 Explain legal frameworks governing cyberspace, including data privacy, intellectual property, cybersecurity, e-commerce, and telecommunications laws.

2 Analyze ethical dilemmas in cyberspace by applying ethical theories to technology use, digital communication, and data handling practices.

3 Apply cybersecurity concepts to identify threats, vulnerabilities, and best practices for protecting digital assets in compliance with legal and ethical standards.

4 Analyze international legal frameworks, treaties, and jurisdictional issues affecting cyberspace and cross-border data activities.

5 Evaluate emerging legal, ethical, and technological developments in cyberspace to adapt to evolving challenges.

Pre-requisite of course: Ethics and Moral Philosophy, Intellectual Property (IP) and Data Privacy, Legal Foundations

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
2	0	2	50	30	20	25	25

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
1	**Introduction to Cyber Law Evolution of Computer Technology** Emergence of cyberspace, Cyber Jurisprudence, Jurisprudence and law, Doctrinal approach, Consensual approach,, Real Approach, Cyber Ethics, Cyber Jurisdiction, Hierarchy of courts, Civil and criminal jurisdictions, Cyberspace-Web space, Web hosting, and web Development agreement, Legal and Technological Significance of domain Names, nternet as a tool for global access.	6
2	**Information technology Act** Overview of IT Act, 2000, Amendments and Limitations of IT Act, Digital Signatures, Cryptographic Algorithm, Public Cryptography,, Private Cryptography, Electronic Governance, Legal Recognition of Electronic Records, Legal Recognition of Digital Signature Certifying Authorities, Cyber Crime and Offences, Network Service Providers Liability, Cyber Regulations Appellate Tribunal Penalties and Adjudication	6
3	**Cyber law and related Legislation** Patent Law, Trademark Law, Copyright, Software – Copyright or Patented,, Domain Names and Copyright disputes, Electronic Data Base and its Protection, IT Act and Civil Procedure Code, IT Act and Criminal Procedural Code.	7
4	**Relevant Sections Act and Procedures** Relevant Sections of Indian Evidence Act, Relevant Sections of Bankers Book Evidence Act, Relevant Sections of Indian Penal Code, Relevant Sections of the Reserve Bank of India Act, Law Relating To Employees And the Internet, Alternative Dispute Resolution, Online Dispute Resolution (ODR)	7
5	**Case Study On Cyber Crimes** Harassment Via E-Mails, Email Spoofing, Cyber Pornography (Ex. MMS), Cyber-Stalking, Introduction: Digital Personal Data Protection Act.	6
Total Hours		**32**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Case Study Analysis on Cybercrime In this practical, students will analyze a real-life cybercrime case such as a phishing attack, ransomware incident, cyberstalking, or identity theft. The objective is to understand the nature of the crime, identify the sections of applicable cyber laws (such as the IT Act 2000 and relevant IPC sections), and evaluate the ethical and legal consequences involved. Students are expected to submit a brief report or presentation explaining their findings and interpretations.	2

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
2	**Practical 2** Drafting a Cybercrime Complaint This activity helps students understand how to formally report a cybercrime. Learners will prepare a mock complaint for a fictional phishing or fraud incident. The complaint should include victim details, a clear description of the incident, the digital evidence available, and the legal sections under which the complaint is being filed. This exercise builds familiarity with the structure and legal language used in cybercrime reporting.	2
3	**Practical 3** Role-Play: Cyber Law Courtroom Simulation Students will participate in a role-play activity simulating a cybercrime court trial. Roles such as judge, prosecutor, defense lawyer, and the accused will be assigned. The case can revolve around issues like defamation, hacking, or data theft. Each group will perform their role based on the facts of the case, following courtroom procedures. A written judgment will also be submitted by the student acting as the judge, based on arguments presented during the trial.	2
4	**Practical 4** Social Media Ethics Audit This practical involves analyzing the ethical aspects of social media use. Students will select two social media profiles (real, with permission, or fictional) and audit their posts for potential issues like cyberbullying, hate speech, misinformation, or data privacy violations. The student must then prepare a report with screenshots (if applicable), identify unethical behavior, and reference the laws or guidelines that relate to the situation.	2
5	**Practical 5** Digital Evidence Collection and Preservation In this practical, students will explore how digital evidence is collected and preserved in accordance with legal standards. The task involves identifying types of digital evidence such as email headers, server logs, or device screenshots. Students will also simulate maintaining a chain of custody to ensure that the evidence is admissible in court. A report documenting the steps taken to collect and preserve the evidence will be submitted.	2
6	**Practical 6** Create a Cyber Ethics Policy for Students Students will draft a cyber ethics policy specifically designed for educational institutions. The policy should contain at least 10 rules that promote responsible digital behavior, covering issues like plagiarism, online harassment, privacy, unauthorized access, and use of school networks. Each rule should be justified with a rationale. This exercise aims to encourage the development of ethical standards within educational environments.	2

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
7	**Practical 7** Legal Analysis of Website Privacy Policies This practical involves selecting and analyzing the privacy policies of two popular websites, such as Facebook, Amazon, or Instagram. Students will study how these websites handle user data, what rights users have, and how the companies comply with data protection laws. The final output will be a comparative report highlighting key legal clauses, user obligations, and whether the policies are compliant with laws like GDPR or the Indian IT Act.	2
8	**Practical 8** Cyberbullying Awareness Campaign Students will conceptualize and implement a campaign aimed at raising awareness about cyberbullying. They may design posters, create short videos, write skits, or organize webinars. The content should define what cyberbullying is, provide real-life examples, mention legal consequences under the IT Act, and explain how victims can report such incidents. The campaign can be conducted within the institution or shared online to maximize reach.	2
9	**Practical 9** Presentation on International Cyber Laws In this activity, students will research and compare cyber laws in India with those of other countries such as the United States (CFAA), United Kingdom (Computer Misuse Act), and European Union (GDPR). They will prepare a presentation that outlines key similarities and differences, and reflect on how India's cyber laws can be improved. This practical encourages global awareness and critical thinking about legal systems.	2
10	**Practical 10** Plagiarism and Intellectual Property Violation Detection This practical teaches students how to detect plagiarism and understand its legal and ethical implications. Students will test different pieces of content using plagiarism detection tools like Turnitin, Grammarly, or online plagiarism checkers. They will evaluate the originality of the content and learn about copyright laws and the concept of fair use. A report will be submitted discussing findings and legal perspectives on intellectual property rights.	2
Total Hours		**20**

Textbook :

1 Cyber Law: Maximizing Safety and Minimizing Risk in Classrooms, Stephen D. Hughes, -, -

References:

1 Ethical and Social Issues in the Information Age, Ethical and Social Issues in the Information Age, Joseph Migga Kizza, Springer, 2010

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

References:

2 "Cyberlaw" The Law of the Internet and Information Technology", "Cyberlaw" The Law of the Internet and Information Technology", Brian Craig, Pearson, 2013

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
0.00	30.00	20.00	22.00	16.00	12.00

Instructional Method:

1 The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

2 The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.

3 Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

4 Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1 "Cyber Law in India" by Pavan Duggal

2 "Cyber Crime Portal" – Ministry of Home Affairs, Government of India https://cybercrime.gov.in/

3 "Cybersecurity and the Law" – Coursera by University of London : https://www.coursera.org/learn/cybersecurity-law